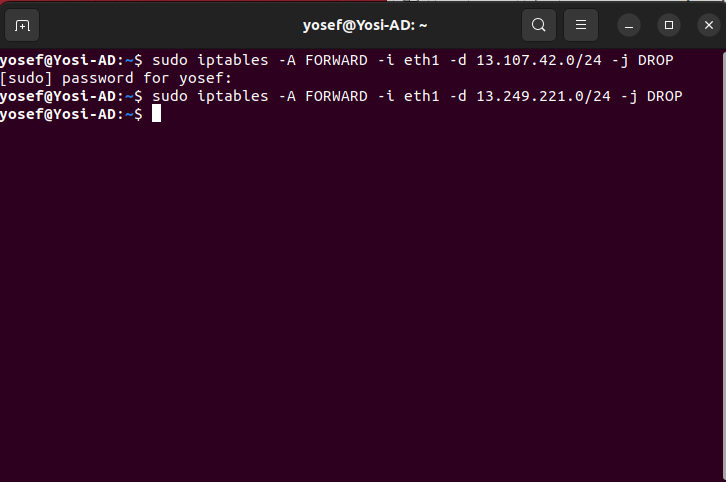
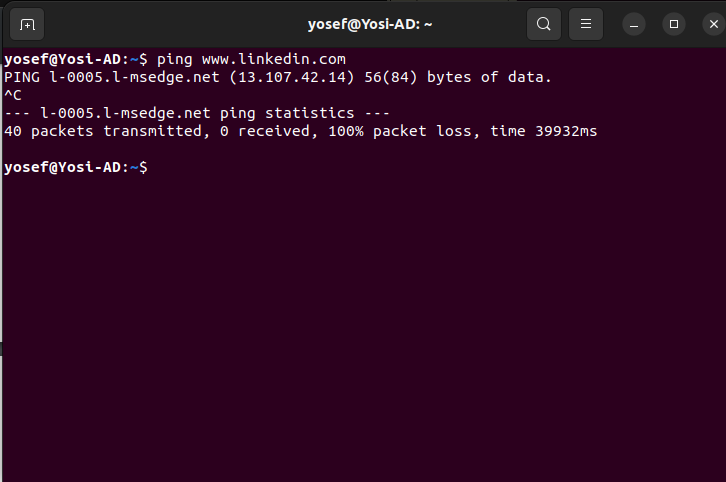
**Task 0 Get Familiar With Lab set**



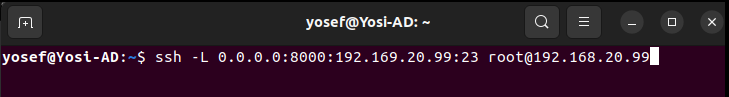
Setting up the rule in Iptables for restricting 2 IP address. Eg: linkedin.com and miniclip.com

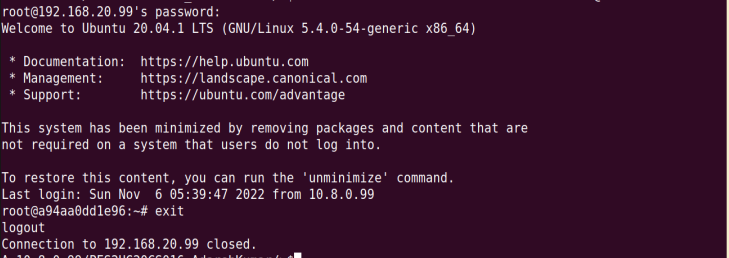


Observation: As we can see that now when we are trying to ping nothing appears on the terminal because they are blocked by the default firewall.

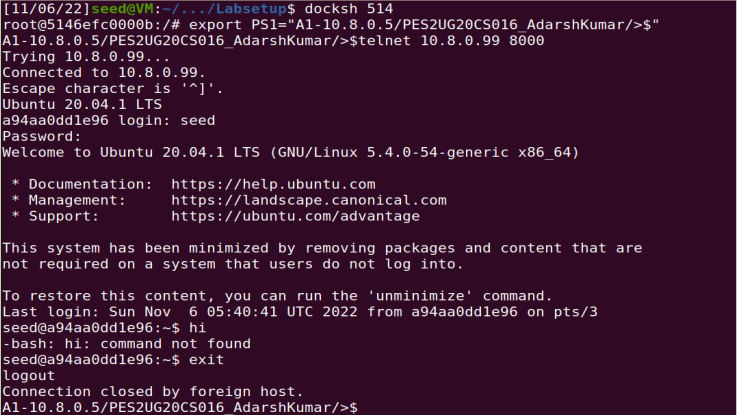
**Task1 : Static Port Forwarding**

On docker container A-10.8.0.99

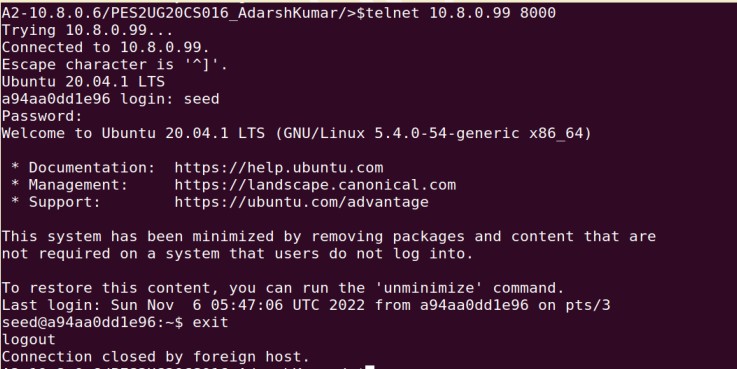




On docker container A1



On docker container A2



We are trying to established a docker telnet connection form docker container A1 & A2

**Questions**

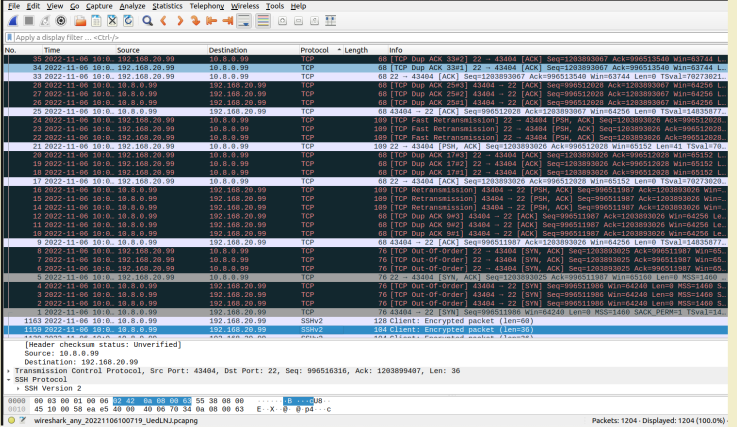
(1) How many TCP connections are involved in this entire process. You should run Wireshark or tcpdump to capture the network traffic, and then point out all the involved TCP connections from the

captured traffic.

**Answer** : 3 TCP connection are involved in this process.

(2) Why can this tunnel successfully help users evade the firewall rule specified in the lab setup?

**Answer** : Yes, we can use this tunnel to evade the firewall rule. As port 23 is blocked but we can see that port no. 22 is still open, from that port we can establish a SSH connection which act as a tunnel between internal host and internal machine.

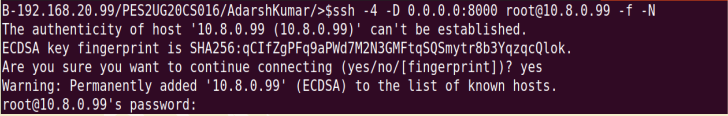


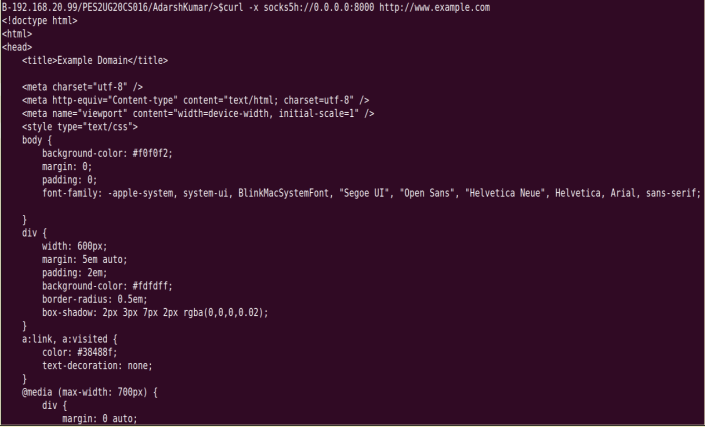
Here we can see that that telnet connection is successfully established between internal host and external host via SSH tunneling mechanism.

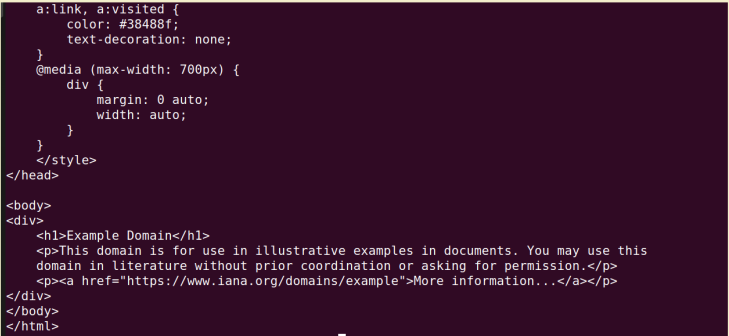
**Task2 : Dynamic Port Forwarding**

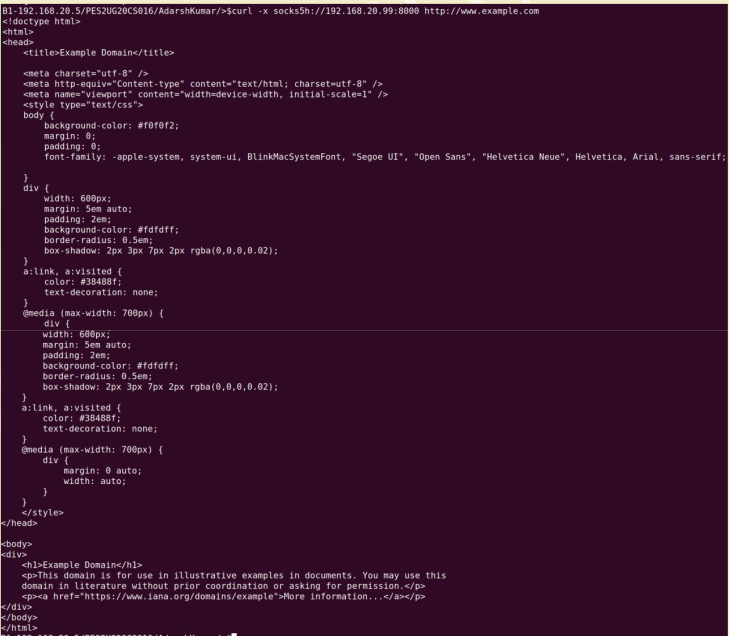
2.1 Setting Up Dynamic Port Forwarding

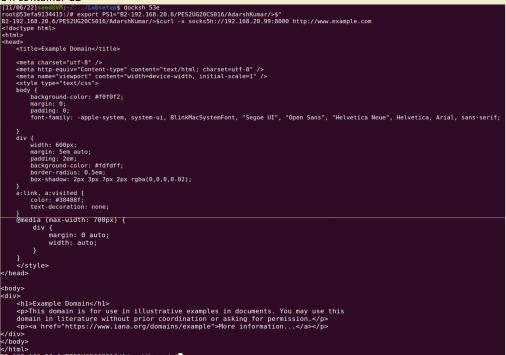
On container B







On container B1



(1) How many TCP connections are involved in this entire process. You should run Wireshark ortcpdump to capture the network traffic, and then point out all the involved TCP connections from thecaptured traffic.

**Answer**: Here the actual connection is established by the external machine A. the internal host indirectly

establish connection via SSH tunnelling.

(2) Why can this tunnel successfully help users evade the firewall rule specified in the lab setup?

**Answer**: The curl commend will be forwarded to the external host to which we have established

connection. That command will be used by the external host to fetch information required and it will

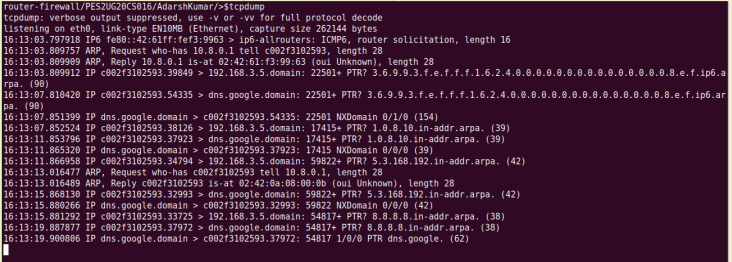
send it to the internal host.

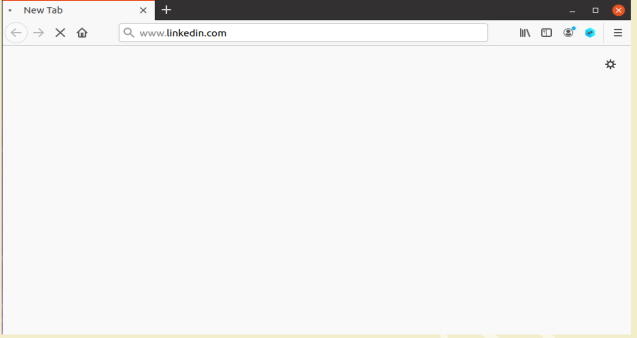
Task 2.2 Testing the Tunnel Using Browser

run tcpdump on the router-firewall, and point out the traffic involved in the entire port

forwarding process.

We can see that packets are being forwarded and the path is clearly visible on the router-firewall

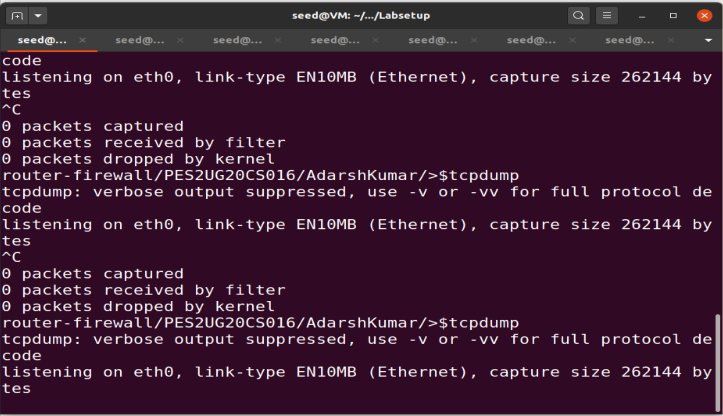




2) Break the SSH tunnel, and then try to browse a website. Describe your observation

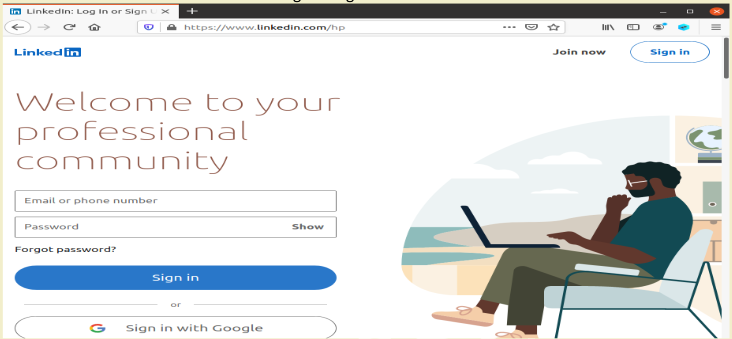
After breaking the SSH tunnel, it shows that the connection is refused because of firewall rules





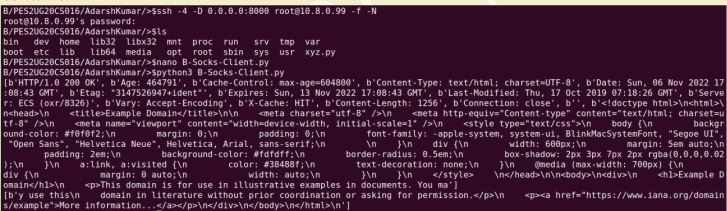
After cleaning up the proxy:

We can see that LinkedIn started working fine again

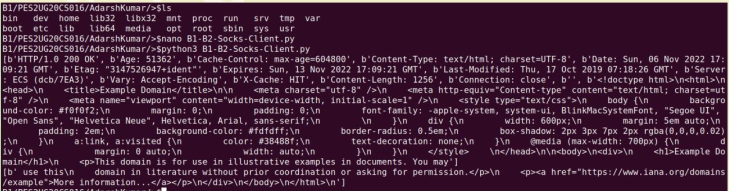


Task 2.3 : Writing a SOCKS Client Using Python

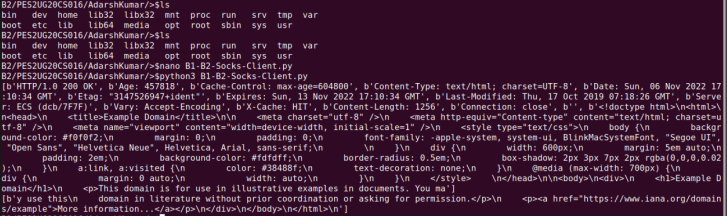
Container B



Container B1



Container B2



Here we can observe that traffic flow and we are able to fetch the content from the net as well.

SSH shell that is in the background



**Task 4: Comparing SOCKS5 Proxy and VPN**

* A SOCKS5 proxy is a more secure alternative to a traditional proxy that protects the traffic within a specific source, such as an application. When you use a SOCKS5 proxy, data packets from the configured source are routed through a remote server.
* This server changes the IP address associated with these data packets before they reach their final destination, offering greater anonymity online.
* SOCKS5 is the most recently optimized version of SOCKS, an internet protocol that funnels web traffic through a remote server.
* Using a SOCKS5 proxy for uTorrent or other P2P app will allow you to achieve better download/upload speeds when compared to VPN.
* While VPN encrypts your traffic, SOCK5 doesn’t.
* In some instances, proxy servers might keep logs. That means if anyone is able to hack those servers, they will be able to obtain logs of your online activities

Difference between SOCKS5 Proxy vs VPN

|  | SOCKS5 Proxy | VPN |
| --- | --- | --- |
| Encryption | SOCKS5 proxies don’t encrypt your data. | VPNs encrypt all your network traffic, ensuring that no one can snoop on your activity. |
| IP Address | SOCKS5 proxies alter your IP address. | VPNs alter your IP address. |
| Speed | SOCKS5 proxies are faster than a VPN because they don’t encrypt your traffic. | VPNs are acutely slower than your normal internet speed, as they encrypt your traffic. |
| Ease of Use | SOCKS5 proxies are manually configured, which is not difficult, but requires some technical knowledge. | VPNs are run from an app downloaded to your device, which makes it extremely easy to use by anyone. |